Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services

Data protection audit report

March 2022

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) inspect and report on the efficiency and effectiveness of Police Forces, other law enforcement bodies and Fire and Rescue Services. HMICFRS have an agreement with the Home Office who provide support for data protection and information governance and as such, HMICFRS have appointed the Home Office's Data Protection Officer as their own to fulfil this statutory function. The Home Office's Office of the Data Protection Officer (ODPO) provide a number of information governance policies and guidance documents for HMICFRS to adopt and amend as necessary. The ODPO also

review personal data breach reports and data protection impact assessments in conjunction with the nominated data protection practitioners at HMICFRS.

HMICFRS agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 29 November 2021 with representatives of HMICFRS to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and HMICFRS with an independent assurance of the extent to which HMICFRS, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of HMICFRS' processing of personal data. The scope may take into account any data protection issues or risks which are specific to HMICFRS, identified from ICO intelligence or HMICFRS' own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of HMICFRS, the nature and extent of HMICFRS' processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to HMICFRS.

It was agreed that the audit would focus on the following area(s)

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UKGDPR and national data protection legislation are in place and in operation throughout the organisation.

Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
Remote Working and Bring Your Own Device	The governance and processes in place for managing personal data which is accessed remotely or through staff members' own devices. This will include controls to monitor hardware issued for remote working, staff owned hardware where company personal data is accessed, access and system controls, risk management and staff training.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid-19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore HMICFRS agreed to continue with the audit on a remote basis. A pre-audit survey was drafted by ICO Auditors and agreed by HMICFRS and launched to HMICFRS staff between 20 January and closed on 14 February. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 7 February to 17 February. The ICO would like to thank HMICFRS for its flexibility and commitment to the audit during difficult and challenging circumstances.

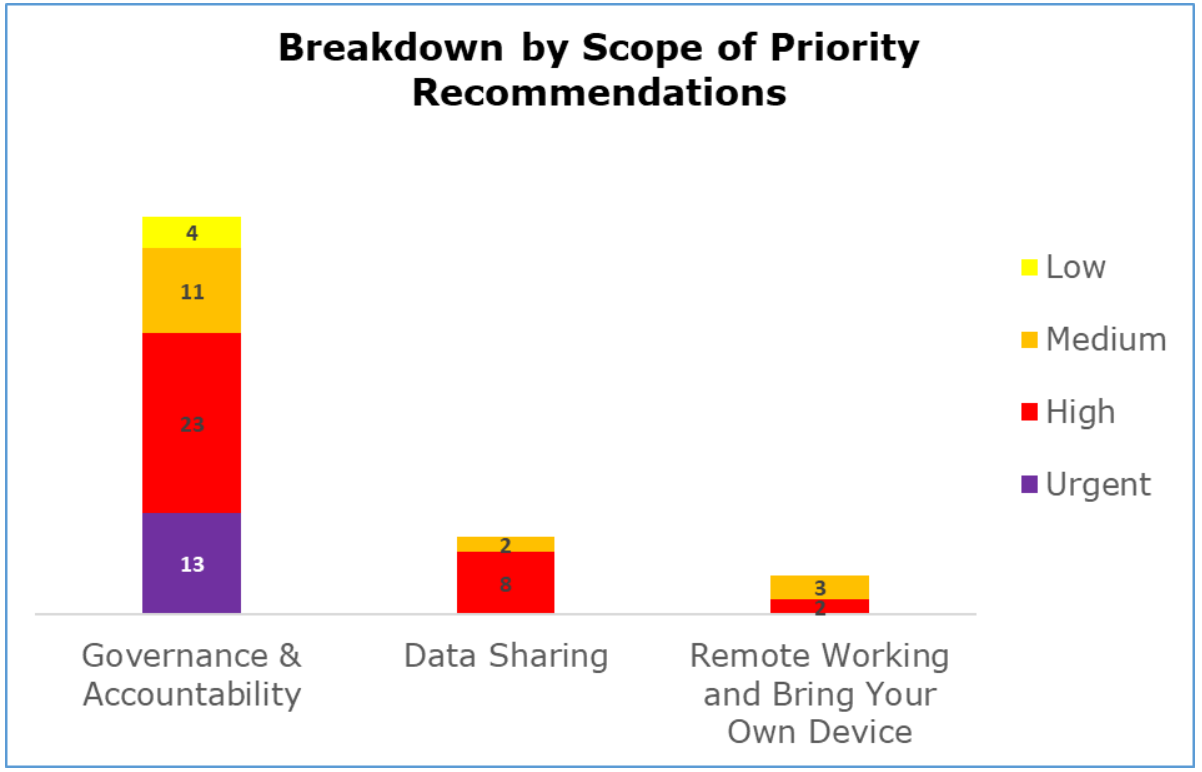
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist HMICFRS in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. HMICFRS' priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Remote Working and Bring Your Own Device	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

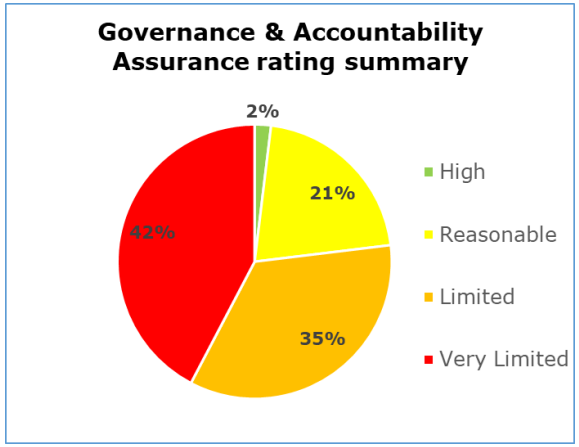


The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

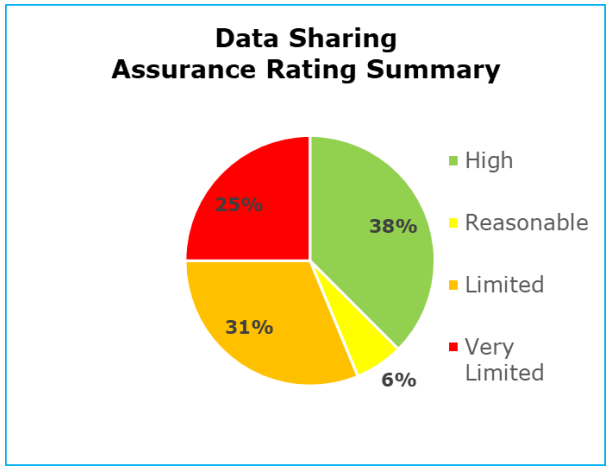
- The Governance and Accountability scope has 13 urgent, 23 high, 11 medium and 4 low priority recommendations.
- The Data Sharing scope 8 high and 2 medium priority recommendations.

- The Remote Working and Bring Your Own Device scope has 2 high and 3 medium priority recommendations

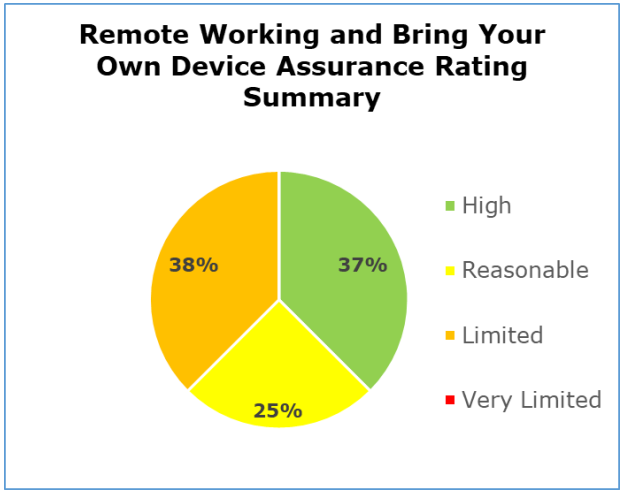
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 2% high assurance, 21% reasonable assurance, 35% limited assurance, 42% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 38% high assurance, 6% reasonable assurance, 31% limited assurance, 25% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Remote Working and Bring Your Own Device scope. 37% high assurance, 25% reasonable assurance, and 38% limited assurance.

Pre-audit Survey

A pre-audit survey was launched to all HMICFRS staff and we received 97 anonymous responses representing around 39% of HMICFRS' employees. The survey consisted of 17 conditional questions which were based on the scope areas covered in the audit and included the following topics; training and awareness, policies and procedures, personal data breaches, bring your own device and remote working.

Areas for Improvement

HMICFRS should: Identify and document a lawful basis for processing for all processing activities, including a Schedule 1 DPA18 condition for processing special category or criminal offence data. Once these bases are identified, develop an Appropriate Policy Document (APD) to support the lawfulness of the processing.

Ensure written contracts are in place with all data processors that process personal information on behalf of HMICFRS. This should be supported by a process that allows HMICFRS to gain assurance that their contracts are established, maintained and reviewed effectively.

Conduct a full data mapping exercise of all processing activities at HMICFRS, to inform HMICFRS' Record of Processing Activities (ROPA). HMICFRS should expand their current ROPA to: include Schedule 1 DPA18 conditions for processing, where appropriate; include adherence to the retention and erasure policies, as outlined in the APD; and increase the granularity of the categories of personal data and recipients.

Establish and document procedural guidance for managing consent. This should include the collection, recording, review and verification of consent. Once approved, these procedures should be made available to staff.

Develop and document the procedure for completing a Legitimate Interest Assessment (LIA) and conduct a LIA for all existing processing activities that rely on legitimate interests.

Review the main privacy information notice to provide specific details about the purpose of processing, the retention period and the lawful basis that is relied upon and what rights are available to the individuals. HMICFRS should be more granular when providing information about the source of the personal information.

Create a HMICFRS specific policy and procedure for the development of memoranda of understanding (MoU) with sharing partners. MoUs should include the security measures and arrangements between sharing partners and controls on the retention and disposal of any personal data. Ensure that all MoUs are centrally logged and reviewed regularly.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services. The scope areas and controls covered by the audit have been tailored to Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.